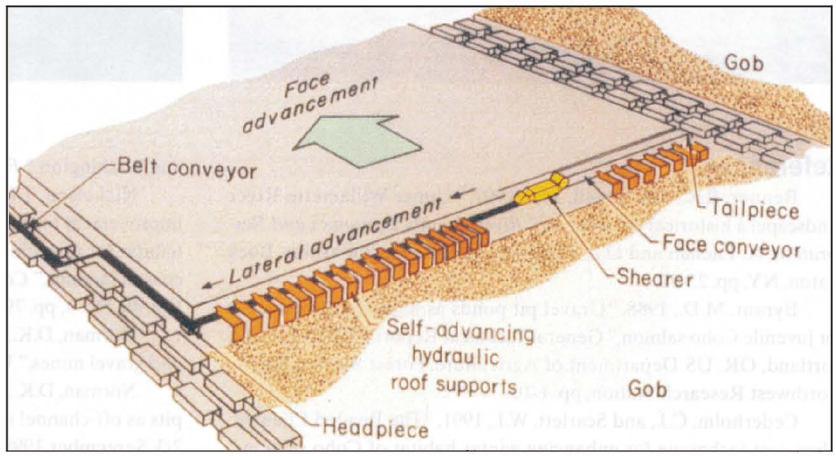
Safety framework for programmable electronics in mining

Mining has one of the highest annual average fatality rates among major US industries. Health and safety dangers have been inherent to mining since the early days of picks and shovels. Even though miners' health and safety has improved over the years, mining is still one of the most dangerous occupations.

Mining was traditionally a low tech industry. It is now driven by competitive pressures to go high-tech by using programmable electronics (PE) for machine control, atmospheric monitoring and material processing. The industry's experience with the functional safety of PE is limited compared with other industries. Thus, PE is an emerging technology for mining that can potentially create or worsen hazards.

FIG. 1

Longwall mining uses a high degree of programmable electronic control.



The US National Institute for Occupational Safety and Health (NIOSH), Pittsburgh Research Laboratory in Pittsburgh, PA is addressing the safety of this new technology. NIOSH has a proactive project to generate recommendations for addressing the functional safety of PE-based mining systems before the technology proliferates. The recommendations take the form of a safety framework encompassing the entire life cycle for a PE-based mining system.

John J. Sammarco

John J. Sammarco is an electrical engineer with the US National Institute for Occupational Safety and Health, Pittsburgh Research Laboratory, PO Box 18070, Pittsburgh, PA 15236-0070.

Approach

The approach to generate recommendations for a safety framework was threefold. Get early industry input, look at current and future trends of PE use for mining and assess the extent of the problem for mining by reviewing mine accident data and general industrial accident data. In addition, an assessment was made of the existing international body of knowledge captured by standards for the functional safety of PE.

Industry input

An industry panel was established in the early project stages to help identify safety issues and to establish initial project direction. This small panel consisted of an industry cross section that included manufacturers, coal operators, academia and government.

The safety issues identified by the industry panel and Sammarco, et al. (1997) involved software, human factors and hardware. Extramural activity was established with The Pennsylvania State University and The University of Alabama to investigate these issues in detail. Additional industry input was obtained by informal contact with manufacturers and end users.

The sampling of industry input indicated an absence of a unified safety approach or a common understanding of the key concepts of PE functional safety concepts. So the first priority task in the safety framework became establishing a common ground and understanding of these key concepts for the mining industry.

Mining trends for PE use

As stated by Phillips, et al. (1997) in the *Wall Street Journal*, "Mining, that most basic of industries, is increasingly throwing down its old tools and picking up new technology. It is a matter of survival."

Informal industry surveys, industry studies and published equipment surveys were used to look at the current state and future trends of PE use. It was found that PE use is not limited to specific systems, mining methods or commodities. In mining, PE use can be categorized in three fundamental areas: control, monitoring and protection.

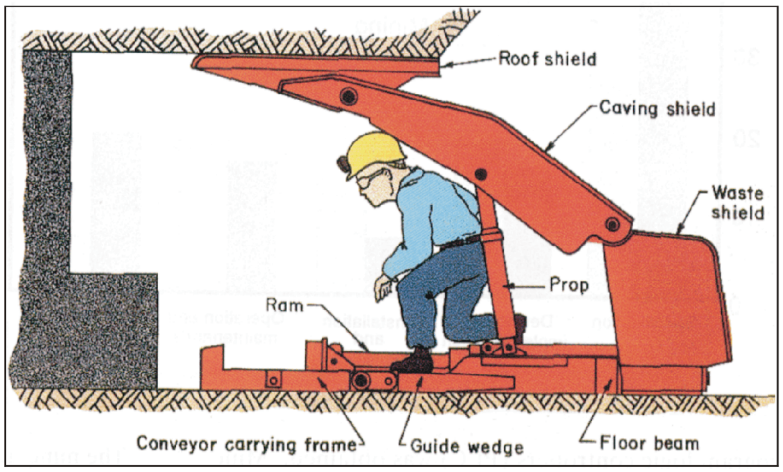
Within these categories, there are several applica-

tions. These include longwall coal mining systems, automated haulage vehicles for surface and underground metal/nonmetal mines, remote controllers for underground mining machines, mine elevators and hoists, and mine atmospheric-monitoring systems that monitor methane, carbon monoxide and fresh airflow.

Underground mine atmospheric monitoring and control began in the late 1970s. It has grown during the 1990s to where almost 17% of all underground mines have computer-based systems (Francart, et al., 1997). From 1990 to 1996, programmable longwall systems usage doubled to about 95% of all US longwalls (Fig. 1) (Fiscor, 1998). Microprocessor technology is also finding its way into control and monitoring of conveyor systems.

FIG. 2

Longwall shield "ghosting" (unexpected) movement is a predominate safety issue.



Industry trends are towards more use and complexity as machinery moves from localized PE control to distributed control of machines and processes. This trend is expected to increase due to economic pressures, lower grades of coal and ores, and because of increased difficulties in physically accessing these resources.

Accident data

Accident data is needed to determine root causes and contributing factors. This information is just one component helping to focus safety recommendations. However, accident data is limited for mining. There are lessons that can be learned from others that have addressed the functional safety of PE. The mining industry will likely repeat some of the same mistakes or have some of the shortcomings experienced by other industries. So NIOSH also looked at studies of accidents in other industries.

Several studies concur that most causes are traced to the safety-requirement specifications for the system. A study by Lutz (1992) on NASA software found that most problems with safety-related software came from misunderstandings and discrepancies in the safety-requirement specifications.

A Health and Safety Executive (HSE) (1995) study of 34 accidents in general industrial applications grouped the accidents by five product life-cycle phases. These included safety requirements specification, design and implementation, installation and commissioning, operation and maintenance, and changes after commissioning. This study found that 44.1% of the causes were attributed to the safety requirement specifications. The second-leading cause (20.6%) was attributed to changes after commissioning.

For mining, a small number of reported accidents was found. This was because PE is an emerging technology in mining and some incidents and near misses go unreported. It is anticipated that incidents will increase as the number and complexity of PE increases for the industry to remain competitive.

Secondly, some accidents caused by PE have gone unrecognized. This is because they are nontraditional and investigative expertise is so strong in the occupational hazards associated with slips and falls, material handling, roof falls, contact with moving machinery and poor work practices.

Accident data obtained from the US Mine Safety and Health Administration (MSHA) — web site http://www.msha.gov/ — has been helpful. MSHA conducts accident investigations of all fatalities but not all accidents or near misses. So it is not known if a large number of uninvestigated PE-related accidents and near misses have occurred.

Using MSHA data, nine accidents were identified. An additional data source concerned mine hoists using

Table 1

Key standards shaping the safety framework.

IEC 61508, parts 1-7	Functional safety of electrical/electronic/programmable electronic safety-related systems.
ANSI/ISA S84.01	Application of safety instrumented systems for the process industries.
ISA draft technical report and TR84.0.02, parts 1-5.	Safety instrumented systems (SIS) — safety integrity level (SIL) evaluation techniques.
MIL-STD-882C	Standard practice for systems safety program requirements.
UK definition standard 00-58	HAZOP studies on systems containing programmable electronics.
STANAG 4404	Safety requirements and guidelines for munition-related safety-critical computing systems.
UL 1998	Software in programmable components.

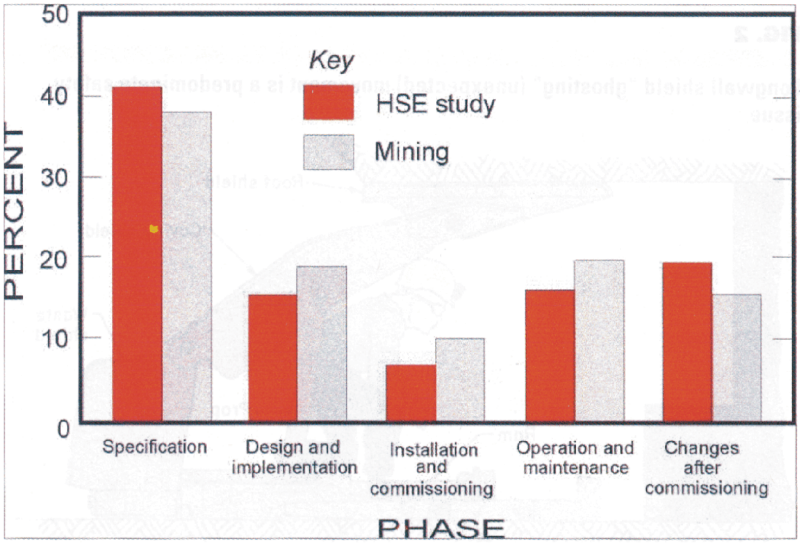


FIG. 3

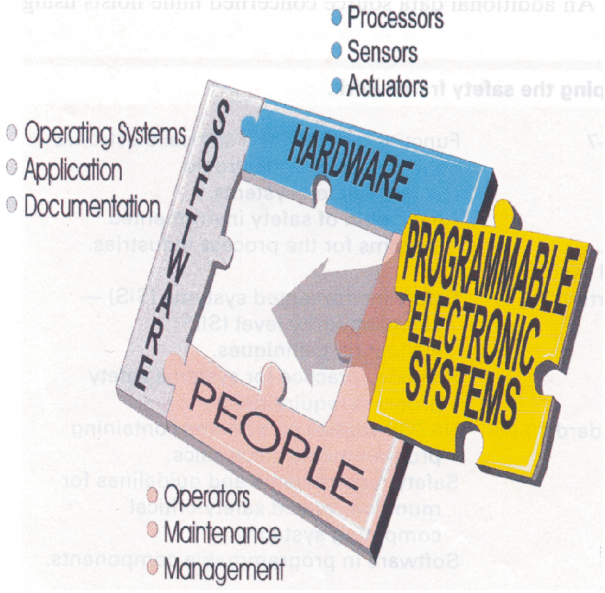
The data analysis from 21 mine accidents shows similarities to the Health and Safety Executive (HSE) study of general industrial accidents involving programmable electronics.

program logic controllers (PLC) was obtained. Mine hoist accident data for 12 accidents from 1987 to 1998 was obtained from the Ontario Ministry of Labor. In all, the data consisted of 21 accidents that were analyzed using the same methodology as the HSE study.

All incidents resulting in injury or fatality involved unintentional or unexpected machine movements. The likelihood and severity of this hazard is greater underground because of the confined space, noise and limited visibility and mobility of workers from awkward body placements and poor floor conditions where obstructions, rubble, water and mud are commonplace. The hazard of unintentional or unexpected machine movement of longwall shields is called ghosting, (Fig. 2). Mishaps and near-misses have occurred because of shield "ghosting." Longwall mining uses PE extensively, where more than 95% of longwall shields use PE control.

FIG. 4

All parts of the mining system must be considered for safety.



The mine-accident-analysis results are compared to the HSE study and are shown in Fig. 3. The predominant cause for mining accidents was the same as found by the HSE study and by Lutz. The safety requirement specification accounted for 38.1% of the data. So the safety framework places emphasis in this area.

Several factors can contribute to a deficient safety requirements specification and implementation. They include inadequate hazard analysis, errors of omission and misunderstandings. Criteria identified by Leveson (1995) are useful for safety requirements specification completeness. The activity driving the specification is the hazard analysis.

Systematic hazard analysis techniques include a hazard and operability study (HAZOP) performed at the requirements phase and continuing into the design, operation and maintenance phases. These could improve the safety requirements specification and mitigate some of the safety problems.

HAZOP began in the chemical process industry. This team-based, qualitative technique uses guide words to discover deviations from the intended design. These guide words are well-suited for process industry parameters, such as flow, pressure, temperature and level.

HAZOP has been extended, as described in the Ministry of Defense (1998), for the hardware and software of programmable systems. Guide words are extended with "early, late, before and after." They are used with attributes such as "data rate and data value."

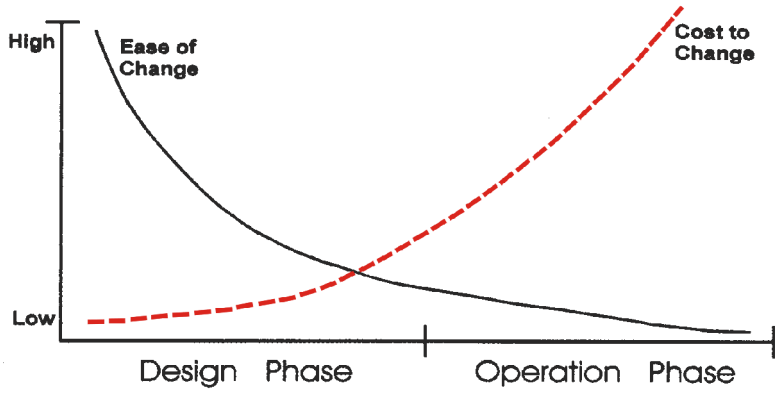
HAZOP is applicable to mining. In fact, Australian law requires a HAZOP study for mining equipment. An extension or customization of HAZOP for mining equipment would be desirable because this involves procedural activities as well as process activities.

Procedural activities for operational sequences involve a combination of people, equipment and the environment. Such a procedural technique, known as Driller's HAZOP, was created for oil-drilling systems (Comer, et al. 1986).

A procedural example in mining would involve a continuous mining machine used to mine coal. This machine spends 32% of the time for production activities, 10% for maneuvering, 42% for delays and idle time and 15% for related personnel activities.

FIG. 5

The impact of change during the development and operational phases.



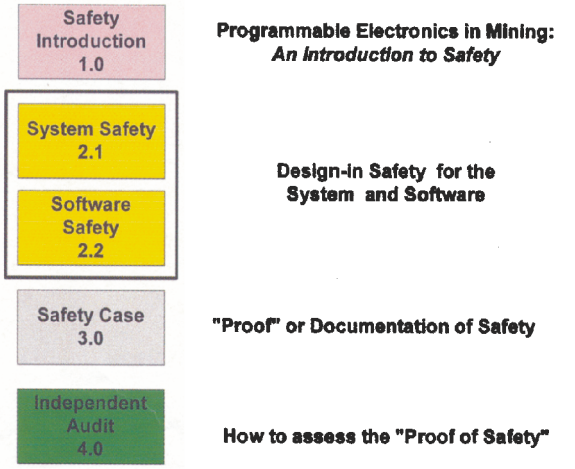
Safety framework

The safety framework is a set of recommendations that addresses the functional safety of PE for mining. It is a risk-based, system safety process. It encompasses hardware, software, humans and the operating environment for the equipment's life cycle. So the safety process considers all parts of the system (Fig. 4). The set of recommendation documents address the life-cycle stages of design, certification, commissioning, operation and maintenance. The safety framework developed by NIOSH is a proactive effort that enables safety to be "designed in" early. This approach enables changes to be made early, thus giving the benefit of lower costs and ease of change (Fig. 5). Changes to the system, once at the customer's site, are more costly and difficult to implement. In addition, software changes in the field can increase the likelihood of introducing new errors.

The mining industry, on a national or international basis, does not have formalized standards addressing the safety of PE. So the safety framework is a first step. It is a practical treatment scaled in size and complexity to small mining organizations that have a few people with limited knowledge of functional safety. The safety framework reflects the importance of having the industry's first steps being manageable and successful. The framework components are as follows (Fig. 6).

FIG. 6

The safety framework.



Safety introduction. This section includes an introductory document for the general mining industry. It provides basic system/software safety concepts. It discusses the need for mining to address the functional safety of PE. And it includes the benefits of implementing a system/software safety program. The document is supplemented by industry workshops. They establish fundamental concepts of system safety, create an awareness of the pending NIOSH safety recommendations and provide a forum for input.

System safety program plan and 2.2 software safety plan. These documents draw heavily from IEC 61508 (1998) and other standards listed in Table 1. The scope is "surface and underground safety-related mining systems employing embedded, networked and nonnetworked programmable electronics."

Safety case and assessment. This defines documentation that demonstrates the degree of safety and the supporting evidence. It also identifies limitations for the system and its operation. It is a "proof of safety" that the system and its operation meet the appropriate level of safety for the intended application. The independent assessment of the safety case is addressed. It establishes consistent methods to determine the completeness and suitability of safety evidence and justifications.

Next steps

The mining industry must have a common understanding of the functional safety concepts presented in the framework for safety. Therefore, the first document concerns the PE functional safety introduction. The concepts of this document will be presented at industry trade association workshops and NIOSH-sponsored workshops. The first such workshop was sponsored by NIOSH and MSHA on Aug. 17, 1999.

Work in 1999 developed technical reports supplementing the safety framework. These reinforced concepts, discussed analysis methods and techniques, and provided examples and additional references. Additionally, a pilot project was explored to implement the safety framework with a mine equipment manufacturer. This could help to refine the safety framework and provide material for case studies.

It is anticipated the framework for safety would be used as the starting point for industry guidance documents or voluntary industry standards that could reduce confusion and establish commonality in the industry. ■

(References are available from the author.)